Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAY 2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Quantum key distribution with high-speed superconducting single-photon detectors	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Institute of Standards and Technology,Division 892,100 Bureau Drive,Gaithersburg,MD,20899**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Technical Digest #QML4.pdf, CLEO/QELS Conference 2007, Baltimore, MD, May 6-11, 2007.

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**2**	

Quantum key distribution with high-speed superconducting single-photon detectors

Robert H. Hadfield[1,2], Jonathan L. Habif[3], Lijun Ma[4], Alan Mink[4], Xiao Tang[4], Sae Woo Nam[1]

[1]*National Institute of Standards and Technology, Division 815, 325 Broadway, Boulder, CO 80305, USA*
phone (303)-497-5309, fax (303)-497-3042, email hadfield@boulder.nist.gov
[2]*Address from January 2007, Department of Physics, Heriot-Watt University, Edinburgh, United Kingdom*
[3]*BBN Technologies, 10 Moulton Street, Cambridge, MA 02138, USA*
[4]*National Institute of Standards and Technology, Division 892, 100 Bureau Drive, Gaithersburg MD 20899, USA*

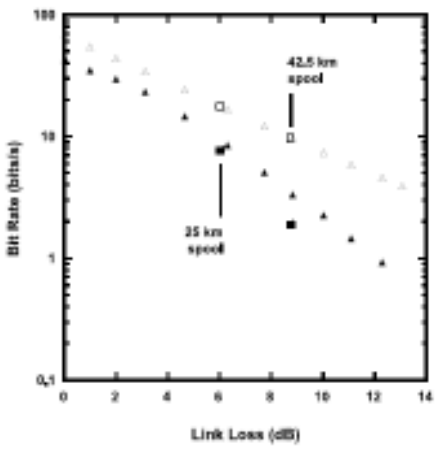
Abstract: We explore the potential of high-speed nanowire superconducting single-photon detectors for quantum key distribution in fiber, over long distances (at 1550 nm) and at high bit rates (at 850 nm).

OCIS Codes: (230.5160) Photodetectors; (270.5570) Quantum Detectors

Single-photon detectors are a crucial enabling technology in Quantum Key Distribution (QKD), the ultimate in secure communications [1]. The ideal detector for this application would have high speed, zero dark counts, and high quantum efficiency at the wavelength of interest. At wavelengths below 1000 nm Silicon Avalanche Photodiodes (Si APDs) are the detector of choice for fiber-based QKD [2,3], with high detection efficiency (~40 % at 850 nm) and low dark counts (~100 Hz). For near-infrared wavelengths such as the standard telecommunication wavelengths (1310 nm and 1550 nm) long transmission distances (up to 122 km) have been achieved through use of InGaAs APDs [4]. These require cooling to 200 K, offer reduced detection efficiency (20-30 %), and are limited to count rates of ~100 kHz. Furthermore, gating is essential to reduce the high dark count rate. Emerging superconducting detector technologies hold promise for QKD. Impressive transmission distances (29 dB link loss - 184 km) have recently been reported using high detection efficiency Transition Edge Sensors [5]. Nanowire-based superconducting single-photon detectors (SSPDs), pioneered by Gol'tsman [6] currently have moderately low detection efficiency (20 % in the visible) and finite dark counts, but are extremely fast (jitter well below 100 ps, recovery time below 10 ns) and offer single-photon counting at very high rates (approaching 1 GHz). Their single-photon counting capability extends well beyond telecommunications wavelengths. In this study we implement SSPDs conveniently packaged in a cryogen-free refrigerator [7], in QKD test beds at 850 nm and 1550 nm.

The first implementation is in a phase-encoding QKD scheme using the BB84 protocol at 1550 nm [8]. The test bed operates using an attenuated laser (mean photon number per pulse $\mu = 0.1$) at a clock frequency of 3.3 MHz. Interferometer stability is maintained via a feedback mechanism. Secret bits are distilled continuously using BBSSS92 privacy amplification [9]. Twin SSPDs are operated at the receiver. The detection efficiency (inclusive of coupling losses) is 0.9 %. The detectors are gated for a 4 ns window each clock cycle, reducing the dark count probability to 4×10^{-7} per clock period. Results are shown in Fig. 1(a). Sifted key transmission rate is shown as hollow points; the distilled secret key as solid points. Transmission loss simulated by digital attenuation is shown as triangles; actual fiber spools (25 and 42 km) are the solid points. In this demonstration, secure transmission is achieved over 12 dB link loss (equivalent to ~60 km of telecommunications fiber). At low link loss, the main contribution to the error rate (QBER) is the modulation error of the interferometer (below 1.5 %). For high link loss, the dominating QBER contribution is detector dark counts. Improving the detection efficiency [10] and narrowing the gating window will lead to improvements in range. With this detector (unlike the alternatives [4,5]) there is potential to increase the clock rate by orders of magnitude, leading to a corresponding improvement in secure transmission rate.

The second implementation is in a polarization-encoding QKD scheme using the B92 protocol at 850 nm [3]. The demonstration was carried out at a clock frequency 625 MHz using attenuated VCSELs. QBER and sifted rates were measured directly; the secret rate was estimated assuming BBSSS92 privacy amplification. In this scheme Si APDs are typically used. Si APDs offer high detection efficiency (40 %), but errors arise from the large detector jitter (400 ps FWHM with an asymmetric tail). This intersymbol interference will cause counts to be erroneously recorded in neighboring clock cycles. At 850 nm, the SSPD has lower detection efficiency (5 %) than the Si APD, but significantly lower jitter (68 ps FWHM with a Gaussian profile) [10]. A histogram of counts recoded on a single



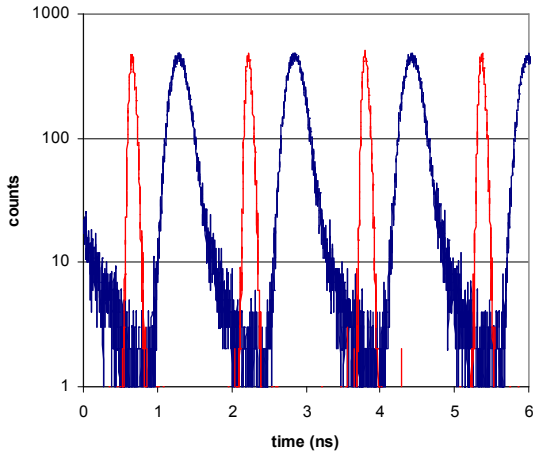


Figure 1(a) QKD at 1550 nm with SSPDs. The sifted rate the hollow points; the secret rate is the solid points. Points where link loss is simulated by attenuators are given by triangles; squares indicate where fiber spools are used.
Figure 1(b) Comparison of detectors under consideration for QKD at 850 nm. Histogram of detection events on a single detector over ~1 s with a return-to-zero repetitive bit sequence at 625 MHz. The SSPD trace is shown in red, the Si APD is shown in blue.

detector channel with a repetitive return-to-zero code recorded at 625 MHz is shown in Fig. 1(b) – note counts are displayed on a logarithmic scale. With any increase in clock frequency, it is clear that in the case of the Si APD, even when bits are selected from a limited time window within each clock period, intersymbol interference will dominate the QBER [2]. The SSPD, in contrast will not be prey to this effect until much higher clock frequencies are reached (approaching 10 GHz) and hence the minimum QBER will be set by the polarization extinction. QBER and sifted rates were measured over 1 km transmission distance at $\mu = 0.1$. Using the Si APD, sifted bits were transmitted at 2 MHz, with a QBER of 3.6 %; using the SSPD, sifted bits were transmitted at 1 MHz with a QBER of 1 % (set by the polarization extinction). Because a larger QBER requires a larger fraction of sifted bits must be used for privacy amplification in order to ensure security, the projected secure key transmission rates using the two detectors are very similar (900 kHz for the Si APD and 830 kHz for the SSPD). For the SSPD, further increases in system clock rate will lead to a corresponding increase in secure rate; for the Si APD this is not true due to intersymbol interference.

In summary, we show that nanowire SSPDs offer many advantages for fiber-based QKD, due to their exquisite timing resolution and low dark counts. We have demonstrated that SSPDs of the current generation are competitive as detectors both for long distance and high bit rate fiber-based QKD. Dramatic improvements in SSPD detection efficiency (up to 57 % at 1550 nm) have recently been reported [11]; these detectors should enable further improvements in the realm of QKD.

The authors acknowledge support from the DARPA QuIST program, the NIST Quantum Information Science Initiative, and DTO. They thank J. Schlafer (BBN), N. Bergren and R. Schwall (NIST) for technical assistance. They also thank G. Gol'tsman for providing the original detectors used in this work.

[1] N. Gisin, *et al.* "Quantum Cryptography," Rev. Mod. Phys. **74,** 145-196 (2002).
[2] K. J. Gordon *et al.* "Quantum key distribution system clocked at 2 GHz," Optics Express **13** (8): 3015-3020 (2005)
[3] X. Tang *et al.* "Experimental study of high speed polarization-coding quantum key distribution with sifted-key rates over Mbit/s," Optics Express **14** 6 2062 (2006)
[4] C. Gobby *et al.* 'Quantum key distribution over 122 km of standard telecom fiber', Applied Physics Letters **84** 19 3762 (2004)
[5] P. A. Hiskett *et al.* 'Long-distance quantum key distribution in optical fibre,' New J. Physics **8** (9) 193 (2006)
[6] A. Verevkin *et al.* "Detection efficiency of large-active-area NbN single-photon superconducting detectors in the ultraviolet to near-infrared," Appl. Phys. Lett. **80,** 4687 (2002).
[7] R. H. Hadfield *et al.* "Single photon source characterization with a superconducting single photon detector,"Optics Express, **13** (26) 10846 (2005)
[8] R. H. Hadfield *et al.* 'Quantum Key Distribution at 1550 nm with twin superconducting single-photon detectors,'accepted for publication, Applied Physics Letters
[9] C. H. Bennett, F. Bessette, G. Brassard, L. Savail, J. Smolin, J. Cryptology **5** 3-28 (1992)
[10] M. J. Stevens *et al.* "Fast lifetime measurements of infrared emitters with low-jitter superconducting single-photon detectors," Applied Physics Letters **89** 031109 (2006)
[11] Rosfjord *et al.* Optics Express **14** (2) 527 (2006)